Memo Issued: July 25, 2008
Control #: MITS-0708-08
Affected IRM: 10.8.1
Expiration Date: 07/31/2009

MEMORANDUM FOR DISTRIBUTION

FROM: /s/ Karen Freeman
Director, Cybersecurity Policy and Programs

SUBJECT: Interim Guidance on *Information Technology (IT) Security Controls for Identification and Authentication*

This interim guidance memorandum is being issued in order to quickly communicate revised security controls, for Identification and Authentication. The revised guidance clarifies account and password policies for all IRS' Applications and Operating Systems (OS). The change(s) are hereby effective immediately for IRM 10.8.1, *Information Technology Security Policy and Guidance; Subsection 10.8.1.5.1, dated March 03, 2008.*

These requirements shall be distributed to all personnel responsible for ensuring that adequate security is provided for IRS information and information systems. The policy applies to all employees, contractors and vendors of the Service.

1. Source(s) of Authority: IRM 10.8.1 is issued under the authority of Treasury Directive (TD) 85-01.

2. Effect on Other Documents:
Internal Revenue Manual (IRM) 10.8 Section 1, Information Technology Security Policy and Guidance, *dated March 3, 2008;*
Internal Revenue Manual (IRM) 10.8 Section 2, Relational Database Management Systems (RDBMS) Security Configurations, *dated February 21, 2008*;
Internal Revenue Manual (IRM) 10.8 Section 6, Secure Application Development, *dated July 07, 2007*;
Internal Revenue Manual (IRM) 10.8 Section 10, Basic UNIX Security Requirements (BUSR) Secure Application Development, *dated October 10, 2007*;
Internal Revenue Manual (IRM) 10.8 Section 20, Windows Security Policy, *dated March 28, 2008;*
Internal Revenue Manual (IRM) 10.8 Section 30, Unisys Operating Systems Security Standards, *dated September 1, 2007;*

Internal Revenue Manual (IRM) 10.8 Section 32, IBM Mainframe System Security Requirements, *dated September 1, 2007;* and
Internal Revenue Manual (IRM) 10.8 Section 42, Web Server and Web Application Server Security, *dated September 14, 2007*.

3. Contact: Please send questions or inquiries related to this guidance, to Janice F. Harrison, Program Manager, Cybersecurity Policy and Procedures Management at (202) 283-6762.

4. Expiration Date: This guidance will be incorporated into the IRM 10.8.1 on or before July 29, 2009

Attachment (1)
Interim Guidance - IRM 10.8.1, *Information Technology Security Policy and Guidance; Subsection 10.8.1.5.1*

Distribution

Chief of Staff, Office of the Commissioner
Deputy Commissioner for Operation Support
Deputy Commissioner for Services and Enforcement
Commissioner, Large and Mid-Size Business Employed Division
Commissioner, Small Business/Self-Employed Entities Division
Commissioner, Tax Exempt and Government Entities Division
Commissioner, Wage and Investment Division
Chief, Agency-wide Shared Services
Chief, Appeals
Chief, Communications & Liaison
Chief, Counsel
Chief, Criminal Investigation
Chief, Equal Employment Opportunity and Diversity
Chief, Financial Officer
Chief, Human Capital Officer
Chief Information Officer
Director, Office of Professional Responsibility
Director, Research, Analysis and Statistics
Director, Office of Privacy, Information Protection and Data Security
Director, Whistleblower Office
National Taxpayer Advocate

cc: IMD Coordinator
Office of Servicewide Policy, Directives, & Electronic Research www.IRS.gov

Attachment (1)

Interim Guidance - IRM 10.8.1, *Information Technology Security Policy and Guidance; Section 10.8.1.5.1*

The following change(s) are hereby effective immediately for IRM 10.8.1, *Information Technology Security Policy and Guidance; Subsection 10.8.1.5.1, dated March 03, 2008.*

CHANGE(s):

10.8.1.5.1
(03-03-2008)
Identification and Authentication

(1) The IRS shall establish, implement, and document a policy and procedure for identifying, authenticating the identity of, and tracking the actions of individuals requiring access to the IRS IT systems.
(2) If several identification and authentication procedures are used, each shall have a separate policy and procedure. At a minimum, the policy and procedure shall:
a. Specify the minimum identification required before issuing credentials.
b. Specify how identity credentials shall be associated with only one individual or process.
c. Specify how identity credentials shall be updated, cancelled, and archived.
d. Specify how identity credentials not associated with an individual (group IDs) shall be controlled, audited, and managed.
e. Specify how identity credentials shall be authenticated (e.g., digitally signed objects, passwords, etc.).
f. Specify how authentication techniques shall be protected against compromise (e.g., password complexity, hardened tokens, etc.).
g. Specify how users are instructed to protect their identity credentials and authentication materials.
h. Specify how often identity credentials shall be renewed/reissued and authentication tokens shall be changed.
(3) User access shall be controlled and limited based on positive user identification and authentication mechanisms.
(4) For IT systems requiring authentication controls, the IT system shall ensure that each user is authenticated before IT system access.
(5) The IRS shall ensure that each person has a unique user identification (ID).
a. MITS shall develop an enterprise method for implementing unique user identification (i.e., Standard Employee Identifier (SEID)).
b. The DAA shall approve the requests for group userids (service accounts).
(6) At a minimum, user IDs and passwords shall be used.
a. Multi-factor authentication shall be used for FIPS 199 categorized high impact information systems.

10.8.1.5.1.1
(XX-XX-XXXX)
Account Management
(X) IRM Sections 10.8.1.5.1.2 through 10.8.1.5.1.X provide security controls for role-base accounts, these security requirements in addition to the account policies stated in section 10.8.1.5.1.8, shall be adhered to for all IRS IT Systems.

10.8.1.5.1.2
(03-03-2008)
Administrator Account

(1) Employees who perform administrator tasks shall have two user accounts - one for administrator duties and one for general user activity (i.e. role-based access).
a. Each account shall be independent of the other, be limited in use, and shall be used solely for its defined purpose. For example, an SA shall not use the SA account to access the employee's own personal files. The various service accounts have specific purposes and shall not be used otherwise.
(2) Administrator accounts shall be prohibited from web browsing and other Internet connections outside of IRS network boundary unless authorized in writing by the CIO or his/her designee.
(3) Administrator accounts shall be prohibited from receiving e-mail from non IRS accounts, unless authorized in writing by the CIO or his/her designee.
(4) Users with administrator access privileges on IRS systems shall access those accounts only from IRS or authorized IRS government contractor systems.

10.8.1.5.1.3
(03-03-2008)
Business Role Account Inactivity

(1) Human accounts shall be disabled, quarantined or removed in accordance with the account polices stated in section **10.8.1.5.1.8.**
(2) A 5081 account deletion request shall be provided for each account to be removed.

SECURITY CONTROLS	ACTION	REQUIREMENT DEFINITION
Disable Account	**45 Days**	After 45 days of inactivity, the account shall be disabled from logging on, but shall not be removed from the system at this time. To be reactivated, the account user shall follow prescribed procedures of the organization responsible for managing the system or application.

Quarantine Account (1)	**90 Days**	After 90 days of inactivity, the account shall remain disabled, and all effective rights of the account shall be revoked. To be reactivated, the account user is required to follow 5081 procedures.
Remove Account	**180 Days**	After 180 days of inactivity, the account shall be removed from the system. To gain access, the account user is required to follow 5081 procedures requesting to be added back.

Notes
(1) All quarantine account implementations shall be approved the Modernization & Information Technology Services (MITS), Information Technology Security Technology Engineering (ITSAE) Organization.

10.8.1.5.1.4
(12-06-2006)
Infrastructure Role Account

(1) The IRS shall remove or disable all infrastructure accounts that are not mandatory. This includes test and default accounts that have no production use.
(2) All vendor-supplied accounts and passwords, including those for software packages and maintenance accounts, shall be changed or disabled as soon as the system or software has been installed.
(3) The super-user account (e.g., root in UNIX, Master in Unisys, etc.) shall be utilized by the least number of staff possible without degrading system availability.

10.8.1.5.1.5
(12-06-2006)
Application Role Account

(1) All vendor-supplied accounts and passwords, including those for software packages and maintenance accounts, shall be changed or disabled as soon as the system or software has been installed. The IRS shall remove or disable all application accounts that are not mandatory. This includes test and default accounts that have no production use.

10.8.1.5.1.6
(12-06-2006)
Fire Call Account

(1) Fire Call procedures shall be implemented for use in an emergency. Fire Call procedures are system specific; consult the appropriate LEMs and IRMs.
(2) For each instance of an installed server (or mainframe) operating system, the local site shall establish, maintain, and control Fire Call accounts for emergency use by Enterprise Operations (EOps) or other approved organizations.
These accounts shall be used for, but not limited to, the following:
a. any of the production server (or mainframe) environments,
b. the Enterprise Computing Center - Martinsburg (ECC-MTB) development environment when the Enterprise Operations (EOps) requests dedicated system time for testing,
c. Disaster Recovery, and
d. other types of users that are identified and documented that shall need occasional use on an emergency or special use basis.
(3) Use of the Fire Call accounts/passwords shall be documented to include the reason for its use and how long it is expected to be used. The use of Fire Call accounts/passwords shall be approved by the site management.
(4) Fire Call accounts shall be locked until management authorizes them to be unlocked.
(5) The Fire Call passwords shall to be placed in a sealed/secured envelope and secured in a lockable cabinet, safe, etc. until use is required.

10.8.1.5.1.7
(03-03-2008)
Service Account Requirements

(1) A service account represents a process or a set of processes to manage authentication service operations with the operating system and/or network resources. A user account is one in which an actual person is assigned.
Some software products (or their configuration for IRS operations) could operate in a non-secure mode with excessive privileges. In some cases this is unavoidable due to the nature of the software product and/or operating system, but in others it is not. The security principle of least privilege shall be adhered to when creating service accounts. System and application owners are responsible for implementing security controls necessary to offset the fundamental security weaknesses/flaws with software/application products. System and application owners shall ensure a full assessment of risk is completed as part of enterprise life cycle processes or as a result of a significant change to the system /application. Below, key requirements are enumerated.
(2) Service accounts shall not be allowed without a documented business need.
a. Use of service accounts shall be based on a full assessment of risk, reviewed by the assigned ISSO and approved by the GSS DAA.

b. All service accounts shall be validated by the System Administrator at least quarterly or as a result of a major change to the system or application to ensure the need for the account is still valid.
c. Elevated privileges assigned to service accounts shall be reviewed by the ISSO. The ISSO shall determine if the request requires a review by MITS Security Engineering and approval by the DAA.
(3) The GSS DAA and application owner(s) shall ensure that service accounts are documented in the SSP and the technical project documentation of the GSS or the Major Application. At a minimum, the application's SSP shall contain the following service account information:
a. System owner, application owner, program/project office, system administrator and POC for maintenance;
b. Written documentation, including business justification, and purpose of the service account;
c. Additional controls necessary to compensate for vulnerabilities and the acceptance of the associated risks; and
d. Identify the architecture including where the service account resides and the targeted servers.
(4) The application owner(s) shall ensure that the assigned SA receives the following support documentation necessary for the administration of the service account:
a. Name of the service account;
b. Purpose of the service account;
c. Service account point of contact (individual's name) - this POC shall:

- be a person who can answer questions about the service account;
- ensure the service account does not inadvertently expire;
- ensure the service account password (if any) is maintained in accordance with password section of this IRM;
- ensure the service account password is at least 14 characters long (based on system capability), but shall be no less than the password minimum length stated in password section of this IRM; and
- ensure the account has documented manager approval.

d. List of users who have administrator rights over the service account; and
e. Manager who authorized the account's existence.
(5) Service account policies and procedures shall include, at a minimum:
a. Naming conventions shall not allow for the indication of the type of service supported and do not use default service account names unless required by the software/application product;
b. Add, change, and delete procedures, at a per-system level and servicewide;
c. Enrollment procedures for grouping (if applicable);
d. Log all service account access/use and review for validation;
e. Quarterly review to ensure the need for the account is still necessary and set up correctly; and
f. Validation of service accounts shall be done at least annually.
(6) The log of all service account access/use shall include, but not be limited to:
a. Date and time of account access;
b. Name of person (or user account) accessing the service account;

c. Date and time service account access is ended; and
d. Date and time service account password was changed.
(7) The number of individuals having access to a given service account shall be based on need to know and the principle of least privilege.
(8) A descriptive identifier shall be created for the service account and noted in the application's SSP and technical documentation. See the applicable OS IRM (Windows, UNIX, or Mainframe) for further information detailing service account information.
(9) User accounts, as defined in the Service Account Requirements section of this IRM, shall not be used as service accounts.
(10) Service accounts shall not be directly logged onto by a user and OS measures shall be used to prevent such local login attempts unless the OS is unable to perform the function.
a. For service accounts that require local logon for system maintenance, the service account shall be disallowed login immediately after system maintenance is performed.
b. The same administrator shall perform and document the process described in requirement a.
c. Service accounts shall not be allowed to operate in a continuous manner with the right to logon locally.
(11) Service accounts shall not be used to perform routine system administration tasks such as adding users or modifying user groups. Implementations that require service accounts to perform such tasks shall thoroughly document the task(s) and the justification for the service account to perform the task(s).
(12) A service account shall not be used outside the defined purpose for which the account was approved.
(13) A service account shall not be accessed by anyone who is not manager approved and in the documented list of users.
(14) Access controls for service accounts shall be implemented in accordance with this IRM.
(15) Auditing for service accounts shall be in accordance with IRM 10.8.3, Auditing Logging Security Standards.
(16) Implementation of service accounts shall be in accordance with the requirements stated above. If necessary, a formal deviation can be submitted in accordance with the process described in the deviation section of this IRM.

10.8.1.5.1.8
(XX-XX-XXXX)
Application and Operating System (OS) Account Policies

SECURITY CONTROLS	AUTHENICATION INDEPENDENT OF OPERATING SYSTEM (OS) (1)	WINDOWS OS (2)	UNIX OS	IBM RACF OS	UNISYS OS
Account	**Forever**	**Forever**	**Forever**	**Forever**	**Forever**

Lockout Duration					
Account Lockout Threshold	**3 Logon Attempts**	**3 Logon Attempts**	**3 Logon Attempts**	**3 Logon Attempts**	**3 Logon Attempts**
Reset Lockout Counter After	**60 Minutes**	**60 Minutes**	**60 Minutes**	**60 Minutes**	**60 Minutes**

Notes
(1) All Applications and Systems where the authentication is not provided by the underlying Operating System. This also includes other device operating systems, such as routers and switches etc.
(2) OMB/NIST Federal Desktop Core Configuration (FDCC) is applicable to any domain configurations that manifest themselves in local FDCC settings.

10.8.1.5.1.9
(XX-XX-XXXX)
Password Management

(1) The IRS shall enforce strong passwords for authentication to IRS IT systems.
(2) The passwords requirements stated in this section are required for all systems, to include the additional requirements stated in section 10.8.1.5.1.10.
(3) IRS users shall not share passwords unless system accounts (e.g., root accounts) must be shared.
(4) Passwords are an important aspect of computer security and are the front line of protection for user accounts. Passwords shall have the following minimum requirements:
a. Passwords shall be required for all accounts. This includes locked accounts where the operating system does not use the password entry to establish the lock.
b. New users shall change the password the first time they log on.
c. Passwords shall not contain any form of the user's name or ID.
d. Service accounts passwords shall expire within 366 days (inclusive).
e. Passwords shall not be kept in plain view.
f. Passwords shall be audited on a regular basis for compliance. This shall be strictly controlled and compromised passwords shall be changed promptly.
g. The system shall not default to displaying a password while logging on.
h. Passwords shall not be displayed in clear text as they are being typed.
(5) The system shall provide a mechanism that notifies the user to change their password.
(6) Forgotten passwords shall be managed in accordance with current Help Desk procedures.

(7) Passwords provided through a procedure that includes another person knowing the passwords (e.g., some help desk password resetting techniques) shall require the owners of the passwords to change them upon initial use when they regain access.
(8) The system, by default, shall not allow the use of null passwords.
(9) Passwords shall not be reusable by the same individual for the same account for a period of at least six months.
(10) All IRS screensaver(s) shall be approved by the Designating Accrediting Authority (DAA).
a. All screen savers used on IRS systems shall be password protected.
b. All IRS systems with screensaver capabilities shall implement a password protected screen saver that automatically locks after 15 minutes of inactivity.
c. Animated screen savers shall not be used on IRS systems. The Logon or “Blank Screen” screen saver is recommended to be used.
(11) To help protect sensitive information or data and the user, the user shall activate the password-protected screen saver, lock his/her workstation, or log off when he/she leaves the machine unattended. To regain access, the user shall be required to enter a unique password or to reboot the system.
(12) Passwords shall be protected from unauthorized disclosure and modification when stored and transmitted.

10.8.1.5.1.10
(XX-XX-XXXX)
Application and Operating System (OS) Password Policies

SECURITY CONTROLS	AUTH NICATION INDEPENDENT OF OPERATING SYSTEM (OS) (1)	WINDOWS OS (2)	UNIX OS	IBM RACF OS	UNISYS OS
Enforce Password History (3)	24 passwords remembered	24 passwords remembered	24 passwords remembered	24 passwords remembered	24 passwords remembered
Maximum Password Age/ Expiration (4)	90 days	60 days	90 days	90 days	90 days
Minimum Password Age (5)	1 day	1 day	1 day	1 day	1 day

Minimum Password Length (6)	**8 characters**	**12 characters**	**8 Characters**	**8 Characters**	**8 Characters**
Password Complexity	Passwords shall not be a word found in a dictionary (even foreign). Passwords shall contain at least one numeric and special character. Passwords shall contain a mixture of at least one uppercase and at least one lowercase letter.				

Notes

(1) All Applications and Systems where the authentication is not provided by the underlying Operating System. This also includes other device operating systems, such as routers and switches etc

(2) OMB/NIST Federal Desktop Core Configuration (FDCC) is applicable to any domain configurations that manifest themselves in local FDCC settings.

(3) Prevents users from toggling among favorite passwords and reduces the chance a hacker/password cracker will discover passwords.

(4) Period of time a user is allowed to have a password before being required to change it.

(5) Period of time a user must wait after changing a password before changing it again.

(6) The minimum length for a password.